CHESTERFIELD COUNTY
ADMINISTRATIVE POLICIES AND PROCEDURES

Department:	**Information Systems Technology**	**Policy Number:**	**7-8**
Subject:	**Internet and E-mail Use**	**Supersedes:**	**11/07/01**
		Date Issued:	**04/15/03**

I. POLICY STATEMENT

The county network, which includes internet and intranet access and the GroupWise and electronic mail (e-mail) systems, is the property of Chesterfield County. Accordingly, the county reserves the right to review any materials transmitted across or stored in computers attached to the network. Any work-related posting to the internet or intranet or GroupWise and e-mail message is a professional communication in your capacity as a county employee. The tone must be professional and the content must be accurate. Every internet posting and e-mail message must be considered the same as a signed letter written on county letterhead.

II. APPLICABILITY

This procedure applies to all full-time and part-time county employees, contractors, and volunteers utilizing county owned computer resources.

III. FILTERING

IST will install and maintain filtering software for all county computers. Internet filtering of county computers is in accordance with the prohibited uses described in Section VI. Exceptions to the filtering requirement may be made on an individual employee basis for appropriate governmental purposes. Department Directors should forward such requests in writing to their respective Deputy County Administrator, identifying the individual employee and/or physical personal computer requesting the exception and the reason the exception is needed. Departments reporting directly to the County Administrator will file the written exception request with the County Administrator. The County Administrator, Deputy County Administrator, Police Chief or Fire Chief shall notify IST to allow unfiltered access once a request is approved. IST will maintain a list of unfiltered personal computers, which shall be periodically audited by Internal Audit. The filtering of county computers does not relieve persons from the requirements specified in this procedure, nor does it provide a defense to violations of this procedure.

IV. SECURITY OF CHESTERFIELD COUNTY COMPUTER RESOURCES

There are three primary threats to the security of Chesterfield County computer resources: (1) system overload; (2) viruses; and (3) access to the system by unauthorized individuals.

In order to prevent system overload, county employees must restrict the use of the following features only for work-related purposes: listservs, which generate a large volume of e-mail, and transmission of e-mail messages to a large number of county employees. County-wide e-mails or GroupWise messages shall not be distributed without the approval of a department director/office administrator or a specified designee.

Users are responsible for the use of their account and should take all reasonable precautions to prevent unauthorized persons from being able to use their account. No one shall use the passwords of others, without permission. All passwords shall be made up of combination of letters and numbers to improve security. Report suspected security breaches immediately to IST.

County data that needs to be protected for governmental business, legal or regulatory reasons must not be posted on the internet or transmitted by internet e-mail.

County employees are prohibited from sending any message or posting any information on the internet,

personal or otherwise, that is contrary to the positions of your department or policies of the county, unless such messages are for the purpose of reporting improper or illegal actions of county employees.

V. PRIVACY

All county owned computer systems, hardware, software, and any related systems and devices are the property of Chesterfield County. These include, but are not limited to, network equipment, e-mail, documents, spreadsheets, calendar entries, appointments, tasks and notes which reside in part or in whole on any county computer system or equipment. Accordingly, information stored on such systems or devices is also county property and subject to review at any time. There is no privacy when using county computer resources, and employees have no expectation of privacy in the use of such resources.

Electronic mail records are accessible by IST staff to support system performance measurement, tuning, and troubleshooting. Additionally, Internal Audit and the Police Department may have reason to review the electronic files of employees. Supervisors also have the authority to inspect the contents of any equipment, files, calendars or e-mail of any subordinates in the normal course of their supervisory responsibilities. Because internet e-mail passes through many computer systems when en route to the recipient, it is accessible by third parties and is not a secure means of communication. When communicating with others, either through the county computer system on the internet or through e-mail, users represent Chesterfield County. The information transmitted or received can be traced and/or reported back to the county.

As with any other data (whether for citizens or employees), computerized information maintained by the county is subject to federal, state and local laws. Any e-mail or other communications initiated on a county device may be subject to disclosure under the Virginia Freedom of Information Act ("VFOIA"), the Privacy Protection Act, and judicial subpoena. Since privacy cannot be assured within the internet e-mail system, confidential information shall not be transmitted by internet e-mail.

VI. USE OF THE INTERNET AND E-MAIL SYSTEM

A. **Acceptable Use** – Employees may use county computer resources to access the internet and transmit e-mail messages at any time for work-related purposes. Subject to the provision herein, employees may use the county computer resources to access the internet or send e-mail messages for appropriate non-work related purposes on personal time in accordance with the conditions governing access to their work areas and personal use of the telephone, as long as there is no effect on public business. Personal time includes breaks, lunchtime and the time before and after work. In areas where employees must share equipment or resources for network access, employees using the resources to fulfill job responsibilities always have priority over those desiring access for personal use.

B. **Prohibited Use** – The following activities are prohibited on county computer resources:

1. Intentionally downloading, accessing, viewing, posting, or transmitting information that is abusive, offensive, harassing, threatens violence, or that discriminates on the basis of race, color, religion, sex, national origin, age, or disability.
2. Intentionally accessing, viewing, downloading, posting, or transmitting sexually explicit material from the internet. Sexually explicit material includes any description of or any picture, photograph, drawing, motion picture film, digital image or similar visual representation depicting nudity, sexual excitement, or sexual conduct of any kind.
3. Operating a business, soliciting money, product advertising, or conducting transactions for personal gain or profit, or gambling.
4. Arranging for the sale or purchase of illegal drugs, alcohol, or firearms.
5. Communication with elected representatives or public or political organizations to express opinions or political issues outside of work-related communications.

6. Solicitation for non-county sponsored organizations or functions.

7. Countywide e-mail or GroupWise messages are prohibited, unless first approved by a department director/office administrator or a specified designee. Such messages shall include a statement indicating the person that authorized the message.

8. Reproduction or transmission of any material in violation of any local, state, U.S. or international law or requirement, including material that does not comply with federal copyright laws and copying or reproducing any licensed software, except as expressly permitted by the software license.

9. Using internet e-mail to transmit identifying information related to confidential matters, including but not limited to criminal/juvenile records, personnel records, or records relating to legal matters unless such information is encrypted.

10. Intentionally creating a computer virus and/or placing a virus on the county's network or any other network. Intentionally drafting, forwarding, or transmitting chain letters.

11. Attempts, whether successful or not, to gain access to any other system or user's personal computer data without the express consent of the other system or user.

12. Using the network, internet, intranet, or GroupWise in any fraudulent manner.

13. Any other use of the network that violates Chesterfield County policies or Code of Ethics.

VII. DISCIPLINARY ACTION FOR VIOLATION OF THIS ADMINISTRATIVE PROCEDURE

A. Any employee who intentionally receives, accesses, views, transmits, or downloads sexually explicit material from the internet on county computer equipment will be disciplined up to and including termination. Sexually explicit material is defined as any description of or any picture, photograph, drawing, motion picture film, digital image or similar visual representation depicting nudity, sexual excitement, or sexual conduct in any form. Persons subscribing to an e-mail list will be viewed as having solicited any material delivered by the list, as long as that material is consistent with the purpose of the list. Likewise, persons conducting a search on the internet will be viewed as seeking any results generated by the search, as long as that material is consistent with the search.

B. Any employee who commits or is convicted of a crime related to the use of county computer equipment shall be terminated.

C. Any employee who violates any other provision of this policy shall be disciplined in the following fashion:

1. Any employee whose use of Chesterfield County's computer resources results in damage to those resources will be required to reimburse the county for the cost of repair and reconfiguration, as well as the hours required for the repair work, and costs associated with replacing necessary hardware or software. Where damage occurs as the result of inadvertent actions, without the intent to cause damage, the employee causing the damage will not be held liable for such damage.

2. In determining the appropriate disciplinary action to be taken against an employee under this policy, supervisors shall apply the standards set forth in the Personnel Policies of the county for appropriate situational discipline (Section 4-2) and shall ensure that the employee Code of Ethics (Section 1-4) is maintained. In addition, supervisors shall consider the nature of the employee's job responsibilities, and the legality or illegality of the violation in determining the appropriate disciplinary action. Discipline may include any of the options contained in Section 4-3 of the Personnel Policies, including, but not limited to:

a. Termination of employment.

b. Suspension of access to e-mail or internet services.

c. Restitution or reimbursement for the hours used to conduct personal business on county computer resources during normal work hours when in violation of this policy.

d. Other disciplinary action(s) as outlined in Chapter 4 of Chesterfield County Personnel Policies.